AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

TARGET DEVICES #1 - #3, CURRENTLY LOCATED AT THE DAYTON SECRET SERVICE OFFICE, 200 W. SECOND ST., STE. 811, DAYTON, OH 45402

Case No. 3:20-mj-573

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized):*

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days *(give exact ending date if more than 30 days:* ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kim Martinez
Applicant's signature

SA Kim Martinez
Printed name and title

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by ____ *(specify reliable electronic means).*

Date: ~~12/15/2020~~ 12-17-20

Judge's signature

City and state: Columbus, Ohio

Chelsey M. Vascura, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF 1. Motorola Moto G Cell Phone Serial Number 35553911070668; 2. Stylo 5 LG Cell Phone Serial Number 8901240132; and 3. Stylo 6 LG Cell Phone Serial Number 354525112011901 CURRENTLY LOCATED AT 200 W. Second St. Ste. 811 Dayton, OH 45402	3:20-mj-573 Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **Kim Martinez**, (hereinafter "Your Affiant") being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your Affiant is a Special Agent with the United States Secret Service, and have been since May 11, 2016. I have completed the Criminal Investigator Training Program and the Customs and Border Protection Officer Training Program at the Federal Law Enforcement

Training Center in Glynco, GA and the Special Agent Training Course at the James J. Rowley Training Center in Laurel, MD. I have also completed additional training courses to include: Basic Investigation of Computer and Electronic Crimes Program at the James J. Rowley Training Center, Business Email Compromise and Ransomware Investigations through the National Computer Forensic Institute, Network Layer 1 & 2 Troubleshooting through Federal Virtual Training Environment, Ports, Protocols, and the OSI Model for Network+, Policies and Best Practices for Network+, and Operational Use of Social Media in the Performance and Learning Management System's online training with the United States Secret Service; IT Concepts, Programming in C, and Symbolic Computations in Mathematics (covering the programming systems Maple and Mathematical) at the University of South Florida; and Basic Computer Skills at Saint Leo University. I am presently assigned the responsibility of investigating violations of federal law, including those violations pertaining to computer fraud, wire fraud, and mail fraud.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of Your Affiant's knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched:

Target Device 1: Motorola Moto G Cell Phone Serial Number 355539110706668;

Target Device 2: Stylo 5 LG Cell Phone Serial Number 8901240132; and

Target Device 3: Stylo 6 LG Cell Phone Serial Number 354525112011901

hereinafter collectively referred to as the "Target Devices." The Target Devices are currently located at 200 W. 2nd St. Ste. 811, Dayton, OH 45402

5. The applied-for warrant would authorize the forensic examination of the Target Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On August 21, 2020 in the Southern District of Ohio, law enforcement officers with the Brookeville Police Department conducted a traffic stop on a blue 1992 GMC pickup truck bearing Ohio registration HUV3297 for failure to signal.

7. Contact was made with the driver of the vehicle, later identified as Kenneth Wilson, and the passenger of the vehicle, later identified as Brandi Sweet.

8. Officers observed that the bed of the truck was full of miscellaneous items. Officers asked Wilson about the items in the bed of the truck, and Wilson told officers that he had cleaned out his storage locker.

9. Sweet told officers that the items were from their (Sweet and Wilson's) storage locker and that they intended to sell them at a flea market.

10. Wilson provided officers with an Ohio State Identification card with the name David Christopher Campbell on it. Wilson told officers that his Ohio driver's license had been suspended. Officers returned to their patrol vehicle to confirm the identities of the individuals in the truck.

11. Officers checked the vehicle's registration and learned that Ohio registration HUV3297 was associated with a red 2006 GMC truck and was registered to an Edwin Humphrey.

12. Officers attempted to return to the blue truck when Wilson put the truck into drive and fled the scene.

13. Officers pursued the truck for a time, but ended the pursuit unsuccessfully due to the speed of the pursuit and the traffic conditions at the time.

14. Later the same evening, officers with the Huber Heights Police Department spotted the blue truck and re-initiated pursuit. During that pursuit the blue truck crashed. Officers from the Brookeville Police Department responded to the crash site.

15. The Huber Heights officers advised the Brookeville Police Department that the blue truck had crashed, and that both the driver and the passenger had fled the crash on foot. Huber Heights officers had taken the passenger, Sweet, into custody, but the driver had successfully escaped. Located near the truck was a purse, in that purse was a cellular telephone, Target Device 1.

16. Brookeville officers interviewed Sweet. Sweet initially identified the driver of the blue truck as David Campbell. Later in the interview, however, Sweet admitted that the driver of the vehicle was Wilson. In Sweet's possession was a cellular telephone, Target Device 2. Also in Sweet's possession was an Ohio driver's license for McKayla Lynn Jordan.

17. Officers learned that the blue truck had been stolen from the Prebco Towing impound lot after having been subject to a tow request from the Preble County Sheriff's

Department when the occupant at the truck at that time (neither Wilson nor Sweet) had been arrested for OVI.

18. Brookeville officers obtained a warrant and searched the blue truck. Among numerous other items located in the bed of the truck, officers found a blue wheel tote containing numerous files. Also in the bed of the truck, officers located a notebook. In the cab of the truck, officers located an additional cell phone near the driver's seat, Target Device 3. Visible on the screen of the cell phone was a message from a "Cody" at the Deerfield Inn at 2871 U.S. 35 West Alexandria, Ohio.

19. Officers contacted the Deerfield Inn at 2871 U.S. 35 West Alexandria. They were informed that the room was rented to a McKayla, but that she was known as "Brandi." Also staying in the room was a Kenneth Wilson.

20. Officers learned that files in the blue wheel tote were employee files of certain former employees of Schaffner Manufacturing. The files contained personal identifying information such as the birth dates, names, and social security numbers of the former employees.

21. The following employee files were recovered:

- Joni Ansel
- Sherman Bailey
- Kenneth Banks
- Richard Brown
- Taisha Brunson
- Victor Carrero-Cuevas
- Marquis Cobbs

- Rachel Cruz
- Alexander Cvjetcanin
- Lonnie Davis
- Marcus Deloney
- Edward Dieterich
- Regis Donahue
- Rodlyn Dunson
- William Fincher
- Cornelius Green
- Synthia Hardin
- Debra Lynn Harris

22. Officers made contact with Osborn Manufacturing, the successor to Schaffner Manufacturing, and learned that the files had been taken in a break-in at a storage unit in Richmond, Indiana on July 29, 2020.

23. The notebook contained several pages of writing. Among those pages is the following information:

- A page which states "Brandi [heart drawing]'s Kenny."

- A list of email addresses and associated names, including: bkaweseome6969@gmail.com (Karen Dey); bkmonalisa69@gmail.com (Mona Lisa); bkrobinhood69@gmail.com (Robin Hood); bkbatman69@gmail.com (Bruce Wayne); bksolid6969@gmail.com (Bonnie Clyde);

karendey208@gmail.com (Karen Dey); bw0025891@gmail.com (Bruce Wayne); monacenter65@gmail.com (Mona Center).

- Underneath bw0025891@gmail.com is the parenthetical annotation "Edward Dieterich." Underneath monacenter65@gmail.com is the parenthetical annotation "Rachel Cruz." Edward Dieterich and Rachel Cruz were the names of two employees whose files were stolen.

- There is an additional email address, mcruz19701970@gmail.com. Included near that email address is the annotation "[XXX] [XX] 2563." This annotation is consistent with the social security number contained in Rachel Cruz's employee file.

- The annotation "2871 US 35 West Alex OH 45381," which is the address of the Deerfield Inn.

24. A subpoena was sent to Google for all email addresses found in the notebook, and select additional email addresses. The returns for that subpoena revealed, *inter alia*:

Email Address	Account Name	Create Date	Terms of Service IP Address
bkawesome6969@gmail.com	*[none]*	8/2/2020	*[none]*
bkbatman69@gmail.com	Bruce Wayne	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
bkmonalisa69@gmail.com	Mona Lisa	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
bkrobinhood69@gmail.com	Robin Hood	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
bksolid6969@gmail.com	Bonnie Clyde	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
buildersrobert@gmail.com	Robert Builders	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
bw0025891@gmail.com	Bruce Wayne	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
karendey208@gmail.com	Karen Dey	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
mrcuz19701970@gmail.com	my shiznit n[****]	8/4/2020	2607:fb90:2b03:8ce4:0:15:87c7:8a01
monacenter65@gmail.com	Mona Center	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
taishabrunson054@gmail.com	Taisha Brunson	8/7/2020	2607:fb90:6240:c5dc:0:d:c9b8:4601

25. Officers also conducted certain additional investigation and learned that Pandemic Unemployment Assistance ("PUA") claims had been made in the names of Taisha Brunson and Rachel Cruz.

26. The claim for Rachel Cruz was filed on August 4, 2020. It provided a mailing address of 2871 U.S. 35, West Alexandria, OH. The associated email address was monacenter650@gmail.com.[1]

27. The claim for Taisha Brunson was filed on August 7, 2020. It provided a mailing address of 2871 U.S. 35, West Alexandria, OH. The associated email address was taishabrunson054@gmail.com.

28. Based on my training and experience, I know that phones typically list device information (such as the associated IMEI, Phone Number, Android or Apple ID) and linked user accounts. The device information, includes for instance the phone numbers associated with the phone, the IMEI, and sometimes even includes the name of the phone as provided by the phone user (such as "JohnDoe's I-phone"). Linked user accounts include account names and handles used to log in to Apps regularly used on the phone, such as email accounts used, or online communication platforms. Both device information and linked accounts are key both for identifying the phone user's location and activities during the crime and for identifying the user of the phone. Device information and linked accounts are typically then the basis of key

[1] A subpoena to Google for that email address returned no results. Results were obtained for the email address monacenter65@gmail.com and are summarized in the table above.

additional investigative steps that allow law enforcement to identify the phone user's location at the time of the crime. For example, once the active phone number used by the suspect is identified, law enforcement can then apply for a cell site warrant, which provides location data on the phone user. This location data could potentially be compared to the IP addresses used to log into the suspected Gmail accounts. Additionally, in this case, it also appears that the users of the phone used it to communicate with individuals associated with the Deerfield Inn at 2871 U.S. 35, West Alexandria, OH, and additional communications may exist on the Target Devices connecting the users of the Target Devices to the addresses used in unemployment claims.

29. Similarly, once an email account or Apple ID is identified, law enforcement may be able to apply for a warrant for location data stored by that online provider, such as Google location records. Additionally, in this case, data stored on the phone may reveal that the user of the phone accessed email addresses used to apply for unemployment assistance benefits using the personal identifying information contained in the stolen Schaffner employee files. In this case, no computers were found with the suspects, further suggesting that the suspects may have used the Target Devices to access email accounts.

30. Based on my training and experience, I know that linked accounts, such as a cell phone number or a related email account, also provide key information to indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, if the phone number associated with the phone is a number frequently used by friends or associates of the suspect to contact him or her, the government's identification of the phone number will assist in proving who was using the phone at the time key activity on the phone occurred. Similarly, your

affiant has regularly seen the suspect's full name be listed in the email address linked to a phone, which clearly helps identify the user of the phone.

31. The Target Devices are currently in the lawful possession of the United States Secret Service. It came into the United States Secret Service's possession in the following way: Brookville Police Department obtained a search warrant for the 1992 blue GMC pickup truck after the pursuit, where the cell phones were located. Brookville Police Department also obtained an Ohio state search warrant on the cell phones. Once the case involving Wilson and Sweet was accepted by the United States Attorney's office, Brookville Police Detective Mark Miller delivered the cell phones to the United States Secret Service Dayton Resident Office. Therefore, while the United States Secret Service might already have all necessary authority to examine the Target Devices, Your Affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the Target Devices will comply with the Fourth Amendment and other applicable laws.

32. The Target Devices are currently in storage at 200 W. 2nd St. Ste. 811, Dayton, OH 45402. In my training and experience, Your Affiant knows that the Target Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Target Devices first came into the possession of the United States Secret Service.

TECHNICAL TERMS

33. Based on my training and experience, Your Affiant uses the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected

to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

34. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, Your Affiant knows that the each of the Target Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

35. In my training and experience, examining data stored on devices of this type can also uncover the location of the user when they used the device. In this case, an examination of

the data stored on the Target Devices may connect the users of those devices to the Deerfield Inn.

36. In my training an experience, examining data stored on the devices of this type can reveal which online applications or websites the user of the device has accessed. In this case, examination of the data stored on the Target Devices may reveal whether the users of those devices have accessed an online portal for PUA or logged in to a Gmail email account.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

37. Based on my knowledge, training, and experience, Your Affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant Your Affiant is applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

40. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, Your Affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. Your Affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of the Target Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

42. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. Your Affiant believes that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Additionally, some of the information related to probable cause in this warrant was obtained through a subpoena that was, itself, subject to a non-disclosure order.

Respectfully submitted,

KIM MARTINEZ
Special Agent
United States Secret Service

17 CMV

Subscribed and sworn to before me
on December 16, 2020:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched:

Target Device 1: Motorola Moto G Cell Phone Serial Number 355539110706668;

Target Device 2: Stylo 5 LG Cell Phone Serial Number 8901240132; and

Target Device 3: Stylo 6 LG Cell Phone Serial Number 354525112011901

hereinafter collectively referred to as the "Target Devices." The Target Devices are currently located at.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Target Devices described in Attachment A that relate to violations of **18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 1028A (aggravated identity theft)** and involve Kenneth Wilson or Brandi Sweet since July 29, 2020, including:

a. any information demonstrating possession, use, or access to the Schaffner employee files for the following individuals:

- Joni Ansel
- Sherman Bailey
- Kenneth Banks
- Richard Brown
- Taisha Brunson
- Victor Carrero-Cuevas
- Marquis Cobbs
- Rachel Cruz
- Alexander Cvjetcanin
- Lonnie Davis
- Marcus Deloney
- Edward Dieterich
- Regis Donahue
- Rodlyn Dunson
- William Fincher
- Cornelius Green
- Synthia Hardin

- Debra Lynn Harris

b. any information related to the use of the identifying information contained in the Schaffner employee files to apply for public benefits, including unemployment assistance;

c. any information related to the user of the device's receipt of public benefits, including unemployment assistance;

d. any information demonstrating the creation of, access to, or use of the following Gmail accounts:

- bkawesome6969@gmail.com
- bkbatman69@gmail.com
- bkmonalisa69@gmail.com
- bkrobinhood69@gmail.com
- bksolid6969@gmail.com
- buildersrobert@gmail.com
- bw0025891@gmail.com
- karendey208@gmail.com
- mrcuz19701970@gmail.com
- monacenter65@gmail.com
- taishabrunson054@gmail.com

e. any information demonstrating the user's residence in, use of, access to, or receipt of mail at the Deerfield Inn at 2871 U.S. 35, West Alexandria, OH.

f. any information recording Kenneth Wilson or Brandi Sweet's schedule or travel from July 29, 2020 to the present;

g. any location data showing the location of the device from July 29, 2020 to the present;

h. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of any relationship between Kenneth Wilson and Brandi Sweet, including:

a. communications over messaging applications and text messages

b. Call logs (including calls via both typical phone calls and App-enabled calling methods, such as Facetime or WhatsApp) showing contact between Wilson and Sweet;

c. Contacts in the contact list related to Wilson or Sweet

d. Photographs and videos showing Wilson or Sweet

4. Information and linked accounts and that can be used to establish the location and identity of the phone user, including the phone's associated IMEI, Phone Number, Android or Apple ID and linked user accounts (including user handles and names for internet and social media applications, such as Google, Instagram).

5. Records evidencing the use of Internet Protocol addresses to access Gmail accounts or apply for public benefits, including unemployment assistance; including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.